Private and Confidential

3E Logic

Information Security Management Handbook

Date Written: June 2025 | Prepared by: Guan Rui

1 Introduction

The company abides by ISO27k, which is a set of internationally recognised standards for information security management.

1.1 Overview of ISO27K

The ISO27k standard is a set of ISO standards for managing the risks affecting or involving both business and personal information. It aims to help protect information assets from harm while enabling their legitimate use.

The management system is a structured framework, a systematic approach to:

- Identify information risks of concern
- Understand and evaluate them
- Treat (avoid, share, mitigate or accept) them appropriately, and
- Ensure the risk treatments are working properly in practice, dealing with changes.

The system reflects the company's **commitment to confidentiality, integrity, and availability** of information, with clear targets set in line with ISO27k standards:

- Confidentiality — Ensure the protection of sensitive information from unauthorized access or disclosure - Zero incidents
- Integrity — Ensure accuracy and reliability of information by preventing unauthorized or accidental modification - Zero incidents
- Availability — Ensure that information and systems are accessible to authorized users when needed - 98% availability

It operates via the "Plan-Do-Check-Act" (PDCA) cycle

Phase	Purpose
Plan	Identify and assess information security risks, define policies, set objectives, and select appropriate controls
Do	Implement and operate the selected controls and processes to manage risks
Check	Monitor and review the ISMS, measure performance, audit controls, and assess compliance
Act	Take corrective actions, update controls, and continuously improve the ISMS based on lessons learned and changing circumstances

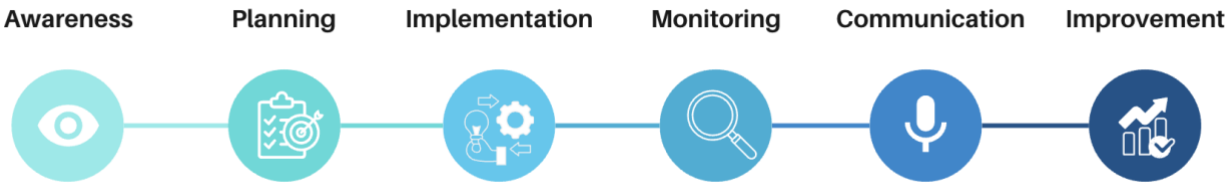
By embedding information security in daily operations, ISO27k helps:

- Protect data across physical, digital, and cloud environments
- Support business goals while managing security risks responsibly
- Build client, partner, and regulator confidence in our ability to safeguard information
- Meet applicable laws, regulations, and contractual obligations

1.2 Sections of Each Clause

To make the ISO 27001 guidance truly usable day-to-day, each clause has been broken down, where relevant—into six practical sections:

1. **Awareness**
2. **Planning**
3. **Implementation**
4. **Monitoring**
5. **Communication**
6. **Improvement**



Awareness highlights the training or reminders you must absorb, ensuring you understand why the control matters and how mistakes can happen**.**

Planning and Implementation spells out the concrete steps and resources you need to put in place up front and take into consideration so you know exactly how to start a control.

Monitoring tells you what to check, log, or review, giving you a clear "keep-an-eye-on-this" list so problems are spotted early.

Communication sets out who to inform and how quickly whenever something looks wrong, preventing surprises and delays.

Improvement explains how to feed lessons learned back into better processes, so the control stays effective and evolves**.**

Together they walk you through planning, doing, checking, and acting (PDCA Cycle) each control while protecting sensitive (employee, customer, supplier) and valuable (IP, financial, legal, operational) information.

1.3 Scope

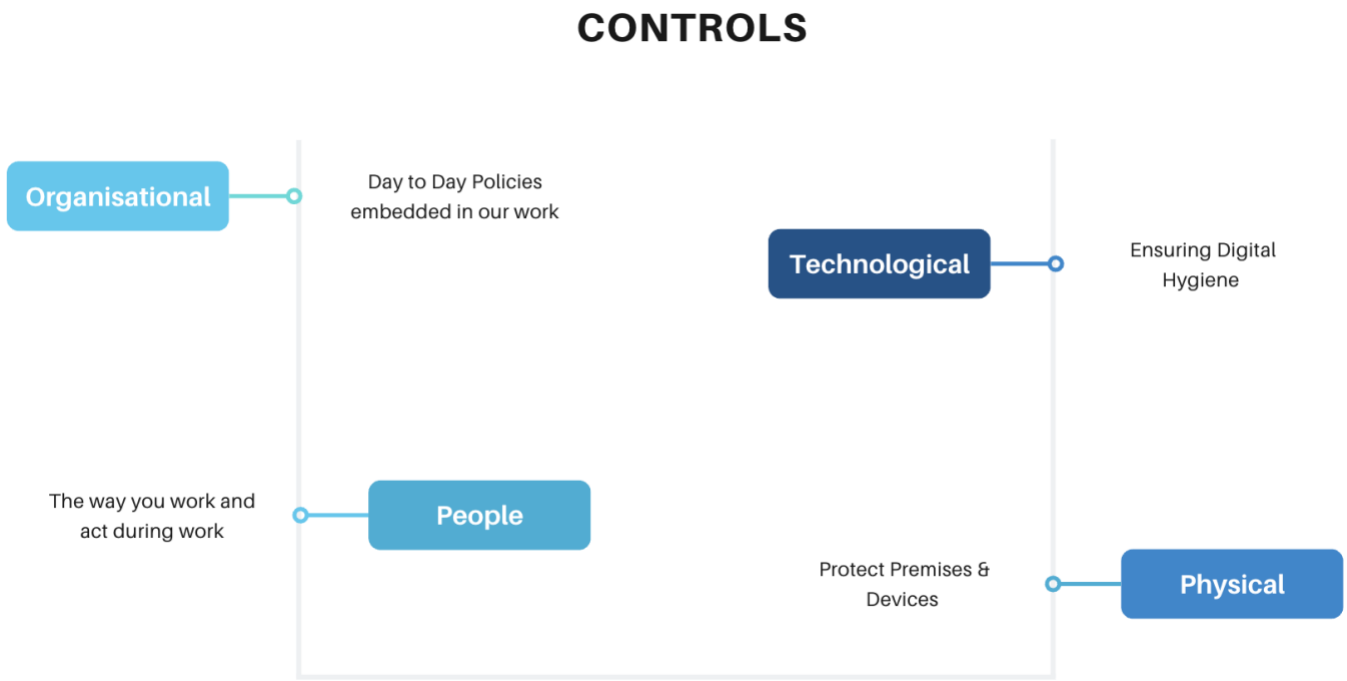
The contents of this handbook apply to:

- **People** – All employees, contractors, and interns working in 3E Logic, whether temporarily or permanently.
- **Assets** – The corporate hard disks, any personal computing devices used in work involving 3ELogic and any cloud storage holding sensitive and valuable data.
- **Activities** – Business operations that collect, process, or store customer, employee, financial, or intellectual-property data, including finance, HR, product development, source codes and IT operations.

1.4 Controls

ISO 27001 groups its safeguards into four controls:

Organisational controls, provides the governance framework. **People controls**, focuses on shaping human behaviour so every worker becomes a dependable line of defence. **Physical controls**, secures buildings, equipment, and media to prevent unauthorised entry or damage; and **Technological controls**, automates protection with tools like firewalls, encryption, monitoring, and backups to keep data safe, accurate, available, and quickly recoverable after an incident.



2 Organizational Controls

Organizational controls are the policies, procedures, and governance processes that ensure information security is embedded in how we work. They ensure every control, be it physical, technological, or people, supports overall business and compliance goals.

2.1 Brief Overview

2.2 Specific Areas

Awareness

- **Role & Responsibilities awareness**
  - Know your role-based security responsibilities
  - You will be held responsible for all activities performed with your User IDs.
- **Compliance –** In consenting with the PDPA, your personal data will be shared, collected and retained by the company unless otherwise stated.
- **Access Control** – Return all assets, and log out of all accounts when your relationship with the company has ended

Planning

- Include security consideration in every phase and process of a project, especially in initiating and planning.
- **Business Continuity Management** – Know the basics of our continuity plan (who to call, where to go, how to work if systems are down).
- **Asset Management** – Identify and document assets important in the operation of projects

Implementation

- **Compliance** – Follow the corporate security policy, code of conduct, and any NDAs.
- **Password Hygiene** – Maintain good password standards. Ensuring that each of these factors are abided by.

Factors	Details
Minimum length	8 characters (letters + numbers)
Change frequency	Every 180 days
History	No reuse of last 3 passwords
Alphanumeric password	Combination of letters and numbers

- **Acceptable Use** – Ensure acceptable usage of software and devices, including personal mobility devices, used for business activities for the company
  - Use licensed software only and handle personal data per PDPA.
  - Keep devices safe, and up to date
  - Avoid performing any actions that may violate copyright laws, such as illegally transmitting copyrighted pictures, software or video.
  - Exercise good judgement to avoid misrepresenting or leaking information about the company to others.
- Document project assets and include security in all project phases.

Monitoring

- **Threat intelligence** – Maintain continuous threat-intelligence and vulnerability monitoring
- **Role Awareness** – Maintain regular manager check-ins when remote.
- Ensure attendance in CISO-led threat-intelligence meeting held twice a year, where findings are reviewed.

Communication

- Report any information security incident to your line manager shall any cyber threat or scam come up.
- **Cloud Services** – When a cloud service is found to be inaccessible for more than 30 minutes, inform CISO or ISO immediately with details such as the directory of the document, title of the document, priority status of the retrieval, and the purpose of the retrieval.

Improvement

- **Reflection & Learnings** – Correlate new vulnerabilities with known threats and act immediately on any that affect company systems.
- Participate in post-incident reviews.

2.3 Resilience Activities

Resilience activities are structured tasks, such as Business Impact Analyses, risk assessments, Business Continuity Plan, and table-top exercises, that ensure the company can withstand, respond to, and recover from any significant disruption.

They identify which processes and resources matter most, establish fallback procedures and recovery targets, and expose gaps before an actual crisis strikes. Because teams understand their own processes, data flows, and pain points the best, accurate insights from employees are often essential. You may therefore be asked to share workflow details, identify potential failure points, or test proposed procedures to ensure the resulting plans are both realistic and effective.

Even if you are not directly involved in creating these resilience plans, you are still expected to read and familiarise yourself with them so that, when a disruption occurs, you can respond quickly and in line with the established procedures.

Activity	What it is	Why it matters	How you may be asked to participate
Business Impact Analysis (BIA)	A structured study that identifies which business processes from various units and assesses the impact and priority if they are disrupted.	It helps the company understand the impact of various scenarios on their work. It pinpoints recovery-time objectives (RTO) and maximum tolerable downtime (MTPD), which drive continuity and disaster-recovery priorities.	• Identify and describe the critical processes in your area, including peak periods and inter-dependencies. • Provide impact estimates (cost, customer, regulatory) if each process is unavailable.
Risk Assessment	The process of identifying threats, vulnerabilities and the likelihood/impact of each scenario, then scoring and prioritising them.	Shows where controls or investments are most urgently needed and in-charge personnel for each follow-up actions.	• Help list realistic threats to your applications or data flow. • Rate likelihood or business impact with domain knowledge. • Suggest practical mitigations for risks.
Business Continuity Planning (BCP)	A documented set of actions and resources that enable essential operations to continue	Minimises downtime, preserves customer trust, and	• Keep local copies of critical procedures or

	or resume quickly after disruption.	meets regulatory obligations.	forms as instructed. • Familiarise with the BCP and know how to call, how to act when disasters strike. • Flag new points of failure so the BCP stays current.
Table-Top Exercises (TTX)	Facilitated "war-game" discussions where a realistic disruption scenario is walked through step-by-step to test BIA, BCP, and incident-response procedures without touching live systems.	Reveals gaps in plans, roles, or communications in a low-risk environment; satisfies ISO 27k and audit requirements.	• Attend the session on time and participate to provide ideas and solutions to solving the issue at each stage. • Identify missing resources or unclear hand-offs so they can be fixed after the exercise.

2.3.1 Risk Assessment Impact

2.3.1.1 Calculations

Marking Scheme	Weight
Risk Level (Customer)	40%
Risk Level (Operation)	30%
Risk Level (Financial)	30%

Impact Level = Impact Level (Customer Satisfaction) x Impact Factor Weight (Customer Satisfaction) + Impact Level (Operation) x Impact Factor Weight (Operation) + Impact Level (Financial) x Impact Factor Weight (Financial)

2.3.1.2 Risk Levels

Risk Level (Customer)	Impact
Very High (4)	Customer will churn / Impact appears in media
High (3)	Customer demands financial compensation
Medium (2)	Customer gives verbal/written complaint
Low (1)	Satisfaction survey affected

Risk Level (Operation)	Impact
Very High (4)	Cost more than 200 man hours; Unable to deliver service and affect safety of environment. Recovery time unknown.
High (3)	Cost 150 - 200 man hours; Affect service delivery. Work around unavailable. Recovery time known.
Medium (2)	Cost 50 - 150 man hours; Slightly affect service delivery; Work around solution available; Recover time known.
Low (1)	Cost less than 50 man hours; No significant impact to operation. Work around solution availability

Risk Level (Financial)	Impact
Very High (4)	Extra expenses more than S$200,000 to rectify
High (3)	Extra expenses between S$100,000 to 200,000 to rectify
Medium (2)	Extra expenses between S$25,000 to 100,000 to rectify
Low (1)	Extra expenses less than S$25,000 to rectify

2.4 Detailed Incident Steps:

2.4.1 Incident Reporting

1. Any issues that affect in information security that may cause a breach must be reported and recorded on event, as well as in Incident and Problem Report.
2. The level of severity of an incident & problem is described in below table and must be referenced during assessment of severity.

Severity	Definition
critical	Incident or Problem which results in a breakdown of business or critical application systems or infrastructure; and led to customer churn.
major	Incident or Problem which result in a partial breakdown of business or critical application systems or infrastructure; and lead to customer complaint.
minor	Incident or Problem which result in no impact to the business, application systems and infrastructure; no customer complaint is received.

Time	Minor	Major	Critical
< 2 hours	No added action required	No added action required	Escalate to Management
4 hours	No added action required	Escalate to Management	Escalate to Management

3. Nature of incident & problem shall be identified.
4. Staff who detects the incident shall prioritise and arrange the corrective action. For IT related issues, report to IT Support for immediate action. Report to director if the incident cannot be resolved in above timeframe. Escalate the incident in accordance to above table.
5. If the incident will impact the customer, should seek action from the customer.
6. If the customer reports the incident, notify the customer of corrective action.
7. All resolutions including root cause, containment and eradication must be recorded on the Incident and Problem Report.

2.4.2 Loss of Cloud Services

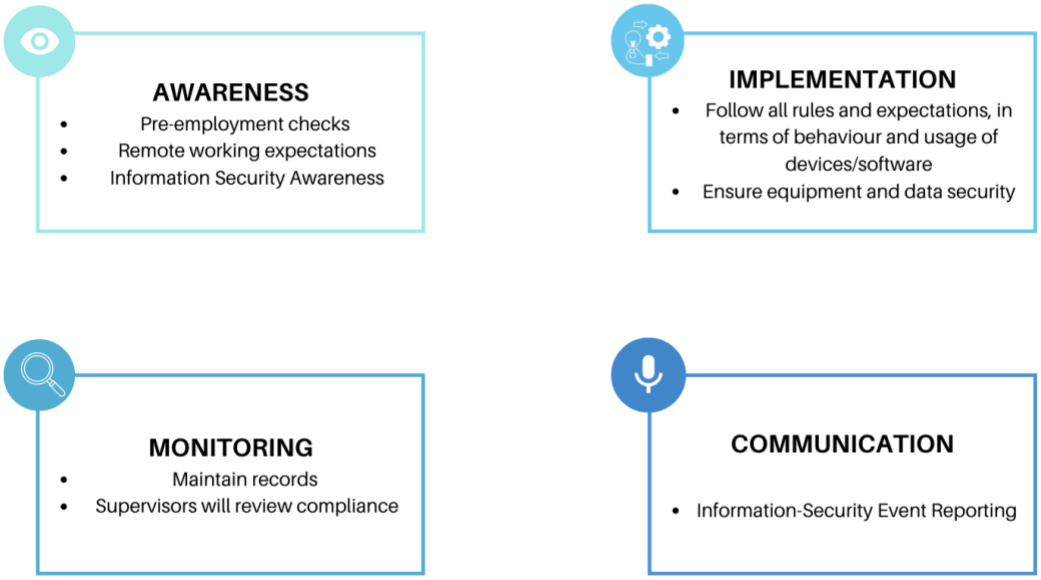
1. When a cloud service is found to be inaccessible for more than 30 minutes, inform CISO or ISO immediately.
2. After either CISO or ISO verified that the cloud services are indeed down, all employees will need to liaise with CISO or ISO directly to request for retrieval of offline backups.
3. Each employee will file a request that include the directory of the document, title of the document, priority status of the retrieval, and the purpose of the retrieval.
   3.1. CISO and ISO will then retrieve the hard disk containing the regular backup files and extract the documents requested by the employees.
   3.2. CISO and ISO will also arrange for the offline transfer of files by either hard drives, thumb drives or any other encrypted means of file transfer.
4. Meanwhile, an appointed IT leader will liaise with the cloud service provider to restore the cloud services as soon as possible.
5. After the cloud services have been successfully restores, all employees must update the files on the cloud server to sync-up any changes made during the breakdown.

Note: The retrieved backup files may not be the latest version. Thus, each employee will have to manually update the relevant parts to the latest version and resume normal business operations from there.

3 People Controls

People control ensure that employees, contractors, and partners understand their responsibilities and act securely.

3.1 Brief Overview



3.2 Specific Areas

Awareness

- **Pre-employment check** – We will conduct background and reference checks in terms of security and integrity you before starting work.
- **Remote working expectations** – The organization is not liable for off-duty incidents, non-work activities, or personal property at your remote location.
- **Information Security Awareness –** You are expected to always follow good security practices, with signed records kept as proof of training.
- You will receive ongoing training or email updates whenever new systems are introduced, reinforced by their managers.

Implementation

- **Follow rules and maintain expectations**
  - Complete security orientation and sign Acceptable-Use & Confidentiality forms.
  - **Equipment usage** – Use company-issued devices/software for work only; keep them updated.

  - **Remote working expectations** – Your duties, performance standards, and agreed working hours remain the same as on-site work, and you must stay in regular, business-hour contact with your supervisor.
  - **Disciplinary process** – Follow all security policies, ensuring a consistent disciplinary procedure
- **Equipment and data security** – Strictly follow software-license terms, keep restricted or sensitive data secure (never copied or removed without approval), and prevent any unauthorized access to systems or information.

Monitoring

- Maintain signed records of training acknowledgements.
- Supervisors will review compliance in team check-ins.
- **Disciplinary process**: Deliberate violations or repeated negligence may trigger disciplinary action, including fines or dismissal

Communication

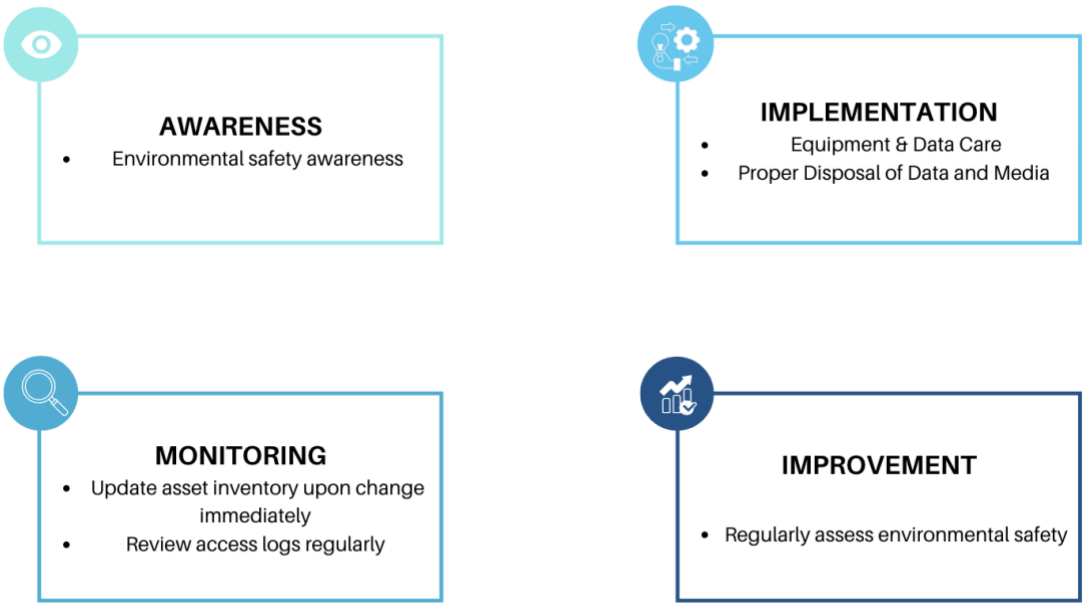
- **Information-Security Event Reporting** – Immediately report suspected vulnerabilities, breach or policy violations via the official channel to enable faster containment, investigation, and recovery.

4 Physical Controls

Physical controls help prevent unauthorized physical access, damage, or interference to physical infrastructure, and information assets. These measures protect not just the technology, but also the environment where information is processed or stored.

Employees play a key role in upholding physical security by following access protocols, securing sensitive materials, and reporting suspicious activity promptly.

4.1 Brief Overview



4.2 Specific Areas

Awareness

- **Environmental safety** – Learn fire-safety and evacuation procedures.

Implementation

- **Equipment & Data care**
  - Lock laptops and portable devices when unattended and store them in secure places.
  - Handle sensitive data only on encrypted hard disks.
- **Data disposal** – Information stored on the equipment should be erased, overwritten, or destroyed in a non-retrievable manner, including all labels and markings which can identify the company

- **Media disposal** – Engage only approved 3rd party company to destruct the media, and keep all media pending for destruction in a locked cabinet

Monitoring

- Update asset inventory when hardware is moved or disposed immediately.
- Review access logs for secure areas periodically.

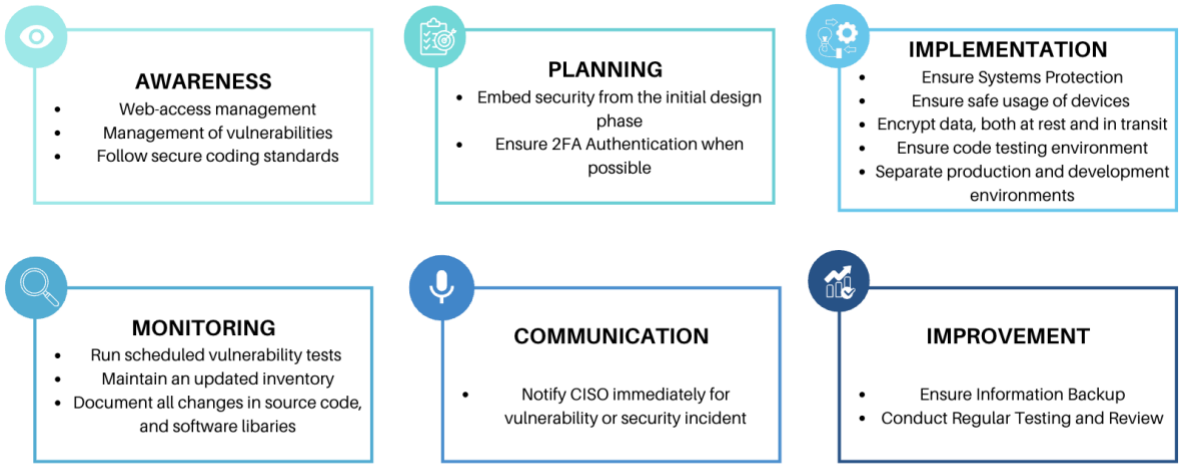
Improvement

- **Environmental safety** – Regularly assess, identify and mitigate risks to critical physical infrastructure due to physical and environmental threats.

5 Technological Controls

Technological controls include software, systems, and technical measures that protect data and networks. These tools block malware, flag suspicious traffic, secure data in transit and at rest, and ensure systems can be restored if compromised.

5.1 Brief Overview



5.2 Specific Areas

Awareness

- **Web-access management** – Access to any blocked site is permitted solely on a documented, legitimate business need and must be explicitly approved.
  - Avoid use of unauthorized software and block traffic to malicious or inappropriate websites.

Blocked Sites	(a) allow information upload
	(b) are confirmed or suspected to host malware/spyware
	(c) are flagged by threat-intelligence feeds
	(d) distribute illegal content

- **Management of Vulnerabilities** – Installation of any unauthorized encryption software is prohibited prior to authorization by management.
- **Secure coding standards** – Follow OWASP Top 10 and related guidelines; use input validation, proper error handling, parameterized queries, and security-enabled frameworks (encryption, authentication) to avoid common exploits.

Planning

- **Secure-by-design**
  - Security should be embedded from the initial design phase, continuing through development, testing, deployment, maintenance, and even retirement.
  - Ensure the implementation of 2FA authentication, if possible, in accordance with clients' requirements and budgets.

Implementation

- **Systems Protection**
  - Keep systems patched and protected by antivirus.
  - Enable Multi-Factor Authentication wherever available.
  - Utilize vulnerability scanning tools to identify vulnerabilities across all computer devices on a periodically basis.
  - Regularly update antivirus software, intrusion detection systems, and other security tools.
- **Safe usage of Personal Computing Devices**
  - Use strong and unique authentication – Set up two-factor authentication when possible and make use of long and complex password.
  - Avoid using the same password across multiple services.
  - Use a trusted private Wi-Fi network or mobile hotspot; avoid unknown public Wi-Fi.
  - Lock the screen when unattended, use a privacy screen in public and never leave devices in plain sight.
  - Think before tapping links in messages or emails.
- **Data Encryption**
  - **Data at rest** – Confidential data at rest on computer systems must be protected by at least one of the following:
    a. Encryption with AES 256 bit or equivalent
    b. Firewalls with strict access controls that authenticate the identity of those individuals accessing the protected data
    c. Complex Passwords or 2 Factor Authentication
  - **Data in transit** – Confidential information transmitted as an email message or through the public network must be encrypted.
- **Outsourced development**
  - Ensure vendors sign the NDA (Non-disclosure agreement) and limit their access to only necessary data.
  - Generate dummy data for testing on third party vendors' side.
- **Testing Environment**
  - Ensure code testing conditions, script are kept constant as production environment.
  - Engage independent testers to perform the acceptance test.

- The development and production environment must be separated and operated in different domain to ensure updates and changes without affect the client side.
- The use of production data in non-production environments should be restricted, unless proper approval has been obtained from senior management and properly deleted from the non-production environments immediately after the test is completed.

Monitoring

- Run scheduled vulnerability scans and report findings.
- Maintain an updated inventory of all hardware, software, and systems in use, including versions and configurations, to facilitate efficient vulnerability identification.
- All changes to source code, and software libraries shall be documented and tracked.

Communication

Notify the CISO immediately whenever you uncover a vulnerability or security incident—for example:

1. Loss or theft of company equipment
2. Issues identified during audit testing
3. Unauthorised changes to source code or software libraries

Improvement

- **Information Backup** – Regularly backup data and information, reviewing the backup log once a month and testing its reliability bi-yearly.
- **Testing & Review** – Run regular peer/automated code reviews, penetration tests, and continuous runtime monitoring; patch promptly when fixes become available and keep developers trained on up-to-date secure-coding practices.

6 Terms and Abbreviations

Abbreviation	Meaning
CISO	Chief Information Security Officer
ISO	Information Security Officer
PDPA	Personal Data Protection Act (Singapore)